IN THE CLAIMS

Upon entry of the present response, the status of the claims will be as is shown below. This listing of claims replaces all previous versions and listings of claims in the present application:

1-33 (Cancelled)

34. (New) A method for protecting a file system in a computer, wherein a user having an access authority for a file can access the file system in the computer, the method comprising:

generating a system security manager's digital signature keys and certificate;

storing the system security manager's certificate onto a security kernel on a server computer;

generating second digital signature keys and a user's certificate;

setting an access authority of the file system;

identifying a user through a digital signature-based authentication when the user attempts to access the file system; and

granting the user access authority for the file in accordance with the identifying result.

35. (New) The method as recited in claim 34, further comprising:

performing a user registering/deleting process when the user is identified as the system security manager.

36. (New) The method as recited in claim 34, further comprising:

setting the access authority of the file system when the user is identified as the system security manager.

37. (New) The method as recited in claim 34, further comprising:

accessing and processing a file.

38. (New) The method as recited in claim 34, wherein generating the system security manager's digital signature keys and certificate comprises:

generating the system security manager's public key;

generating the system security manager's secret key; and

generating the system security manager's certificate.

39. (New) The method as recited in claim 34, wherein identifying the user through a digital signature-based authentication comprises:

generating, at a server computer, random numbers;

generating a digital signature to the random number;

extracting the system security manager's public key from the system security manager's certificate stored on the security kernel;

verifying the user's certificate using the extracted system security manager's public key;

extracting the user's public key and the access authority in the user's certificate; and

verifying the digital signature to the random number.

40. (New) The method as recited in claim 34, wherein granting the user the access authority comprises:

providing the user with the access authority to the file system when the user is a general user; and

providing the user with registering/deleting authority, file system access setting authority and the file system access authority.

41. (New) The method as recited in claim 35, wherein performing the user registering/deleting process comprises:

determining whether user registration or deletion is selected;

deleting data related to a user to be deleted when the user deletion is selected;

registering a user when the user registration is selected;

wherein registering the user comprises:

providing the user to be registered with the access authority;

generating a secret key and a public key of the user to be registered;

generating a certificate of the user to be registered;

encrypting and storing the secret key of the user to be registered; and

storing the certificate of the user to be registered.

42. (New) The method as recited in claim 41, wherein the certificate is generated by encrypting the access authority and the user's public key.

43. (New) The method as recited in claim 36, wherein setting the access authority comprises:

selecting a file;

selecting a user allowed to access the file; and

setting the access authority to the file as an access authority of the user.

44. (New) The method as recited in claim 37, wherein accessing and processing the file comprises:

receiving a name of a file to be accessed;

determining whether an access authority of the file to be accessed is equal to that of the system security manager;

permitting the file to be accessed when the access authority of the file to be accessed is equal to that of the system security manager;

determining whether the access authority of the file to be accessed is equal to that of the user trying to access thereto; and

permitting the file to be accessed when the access authority of the file to be accessed is equal to that of the user trying to access thereto.

45. (New) An apparatus for protecting a file system in a computer system, wherein a user having a file access authority can access the file system in the computer system, the apparatus comprising:

a generator that generates a system security manager's digital signature keys and certificate;

a storage that stores the system security manager's certificate onto a security kernel on a server computer;

a generator that generates a user's digital signature keys and a user's certificate;

an access setter that sets an access authority of the file system;

an identifier that identifies a user through a digital signature authentication when the user tries to access the file system; and

an authorizer that grants the user the access authority for the file in accordance with the identification result.

46. (New) The apparatus as recited in claim 45, further comprising:

a registrar/deleter that performs a registration/deletion of the user when the user is identified as the system security manager.

47. (New) The apparatus as recited in claim 45, further comprising:

an access setter that sets the access authority of the file system when the user is identified as the system security manager.

48. (New) The apparatus as recited in claim 45, further comprising:

an accessor that accesses a file and a processor that processes the file.

49. (New) The apparatus as recited in claim 45, wherein the generator that generates the system security manager's digital signature keys and system security manager's certificate comprises:

a generator that generates a system security manager's public key;

a generator that generates a system security manager's secret key; and

a generator that generates a system security manager's certificate.

50. (New) The apparatus as recited in claim 45, wherein the identifier comprises:

a generator that generates, at a server computer, random numbers;

a generator that generates a digital signature to the random number;

an extractor that extracts a system security manager's public key from a system security manager's certificate stored on the security kernel;

a verifier that verifies a user's certificate using the extracted system security manager's public key;

an extractor that extracts a user's public key and the access authority in the

user's certificate; and

a verifier that verifies the digital signature to the random number.

51. (New) The apparatus as recited in claim 45, wherein the authorizer comprises:

a provider that provides the user with the file system access authority to the file system when the user is a general user; and

a provider that provides the user with registering/deleting authority, file system access setting authority and the file system access authority.

52. (New) The apparatus as recited in claim 46, wherein the registrar/deleter comprises:

a determiner that determines whether user registration or deletion is selected;

a deleter that deletes data related to a user to be deleted when the user deletion is selected;

a registrar that registers a user when the user registration is selected;

wherein the registrar comprises:

a provider that provides the user to be registered with the access authority;

a generator that generates a user's secret key and public key to be registered;

a generator that generates a user's certificate to be registered;

an encrypter that encrypts the user's secret key to be registered and a storage that stores the user's secret key to be registered; and

a storage that stores the user's certificate to be registered.

53. (New) The apparatus as recited in claim 52, wherein the user's certificate is generated by encrypting the access authority of the user and user's public key.

54. (New) The method as recited in claim 47, wherein the access setter includes:

a selector that selects a file;

a selector that selects a user allowed to access the file; and

an access setter that sets the access authority to the file as an access authority of the user.

55. (New) The method as recited in claim 48, wherein accessor and processor comprise:

a receiver that receives a name of a file to be accessed;

a determiner that determines whether an access authority of the file to be accessed is equal to that of the security manager;

a permitter that permits the file to be accessed when the access authority of the file to be accessed is equal to that of the security manager;

a determiner that determines whether the access authority of the file to be accessed is equal to that of the user trying to access thereto; and

a permitter that permits the file to be accessed when the access authority of the file to be accessed is equal to that of the user trying to access thereto.

56. (New) A computer readable media storing instructions for executing a method for protecting a file system in a computer, wherein a user having an access authority for a file can access the file system in the computer, the computer readable medium comprising:

a first generating code segment that generates a system security manager's digital signature keys and certificate;

a storing code segment that stores a system security manager's certificate onto a security kernel on a server computer;

a second generating code segment that generates second digital signature keys and a user's certificate;

an access setting code segment that sets an access authority of the file system;

a user identifying code segment that identifying a user through a digital signature-based authentication when the user tries to access the file system; and

an access granting code segment that grants the user the access authority for the file in accordance with an identification result.

57. (New) The computer readable media as recited in claim 56, further comprising:

a registering/deleting code segment that performs a user registering/deleting process when the user is identified as the system security manager.

58. (New) The computer readable media as recited in claim 56, further comprising:

an access setting code segment that sets the access authority of the file system when the user is identified as the system security manager.

59. (New) The computer readable media as recited in claim 56, further comprising:

an accessing code segment that accesses a file and a processing code segment that processes a file.

60. (New) The computer readable media as recited in claim 56, the first generating code segment comprising:

a public key generating code segment that generates a system security manager's public key;

a secret key generating code segment that generates a system security manager's secret key; and

a certificate generating code segment that generates a system security manager's certificate.

61. (New) The computer readable media as recited in claim 56, the user identifying code segment comprising:

a random number generating code segment that generates, at a server computer, random numbers;

a digital signature generating code segment that generates a digital signature to the random number;

a public key extracting code segment that extracts a system security manager's public key from the system security manager's certificate stored on the security kernel;

a certificate verifying code segment that verifies a user's certificate using the extracted system security manager's public key;

a public key and access authority extracting code segment that extracts a user's public key and the access authority in the user's certificate; and

a signature verifying code segment that verifies the digital signature to the random number.

62. (New) The computer readable media as recited in claim 56, wherein the access granting code segment comprises:

an access authorizing code segment that provides the user with the file system access authority to the file system when the user is a general user; and

a registering/deleting authority code segment that providing the user with registering/deleting authority, file system access setting authority and the file system access authority.

63. (New) The method as recited in claim 57, wherein the registering/deleting code segment comprises:

a determining code segment that determines whether user registration or deletion is selected;

a deleting code segment that deletes data related to a user to be deleted when the user deletion is selected;

a registering code segment that registers a user when the user registration is selected;

wherein the registering code segment comprises:

an access authorizing code segment that providing the user to be registered with the access authority;

a user key generating code segment that generates a secret key and a public key of the user to be registered;

a certificate generating code segment that generates a certificate of the user to be registered;

an encrypting and storing code segment that encrypts and stores the secret key of the user to be registered; and

a storing code segment that stores the certificate of the user to be registered.

64. (New) The computer readable media as recited in claim 63, wherein the certificate is generated by encrypting the access authority and user's public key.

65. (New) The computer readable media as recited in claim 58, wherein the access setting code segment comprises:

a file selecting code segment that selects a file;

a user selecting code segment that select a user allowed to access the file; and

an access authority setting code segment that sets the access authority to the file as an access authority of the user.

66. (New) The computer readable media as recited in claim 59, wherein the accessing and processing code segment comprises:

a name receiving code segment that receives a name of a file to be accessed;

a first access determining code segment that determines whether an access authority of the file to be accessed is equal to that of the system security manager;

a permitting code segment that permits the file to be accessed when the access authority of the file to be accessed is equal to that of the system security manager;

an second access determining code segment that determines whether an access authority of the file to be accessed is equal to that of the user trying to access the file; and

an access permitting code segment that permits the file to be accessed when the access authority of the file to be accessed is equal to that of the user trying to access the file.